REMARKS

Favorable reconsideration of this application is respectfully requested.

Claims 1-24 are pending in this application. Claims 1-24 were rejected under 35 U.S.C. § 103(a) as unpatentable over "Bluetooth Specification", Bluetooth Security, November 29, 1999, pages 149-178 (herein "Bluetooth") in view of "5C Digital Transmission Content Protection White Paper" Revision 1.0, July 14, 1998, pages 1-13 (herein "5C White Paper"), and further in view of U.S. patent application publication 2003/0093669 to Morais et al. (herein "Morais").

Addressing the above-noted rejection, that rejection is traversed by the present response.

Applicants traverse, as discussed in further detail below, the outstanding rejection as the newly cited reference to Morais does not disclose the feature added to the claims in the previous Amendment filed February 7, 2007.

Specifically, independent claim 1 was previously amended to recite:

> wherein at least one of the second authentication unit and the second key exchange unit rejects its process of at least one of authentication and key exchange with the receiving device when at least one of the first authentication by the first authentication unit and the first key exchange by the first key exchange unit with the receiving device is unsuccessful.

That subject matter is fully supported by the original specification for example at page 23, lines 2-14 and Figure 6, steps S37, S38. The other independent claims are similarly amended.

Applicants respectfully submit the claims as currently written distinguish over the applied art as the claims recite specific operations of how first and second encryption keys are utilized to transmit copy protected contents data securely, and such specific combined usage of the first and second encryption keys is not taught or suggested by the combination of teachings in the Bluetooth reference, the 5C White Paper, and Morais.

One objective of the present invention is to provide enhanced transfer of copyright protected contents data, and to particularly realize a secure copyright protection even in a radio network environment.[1]

With reference to Fig. 1 in the present specification as a non-limiting example, the present invention can be applied to a radio communication system including a portable MPEG4 player 101 and a portable viewer 102, which are both owned by the same person and thus that are authorized to communicate information with each other. The portable MPEG4 player 101 and the portable viewer 102 are located within an area in which a connection by a local area radio network is possible. Further, another portable viewer 103 owned by a different entity may also enter that local area, but the claimed system prevents that other portable viewer 103 from viewing data from the portable MPEG4 player 101 as the other portable viewer 103 is owned by a different entity and does not have authorization to view data provided from the portable MPEG4 player 101.

As shown for example in Figure 5 in the present specification at steps S1-S19, a first authentication is carried out to determine whether two devices can properly communicate with each other, such as devices 101 and 102 in Figure 1 in the present specification (steps S1-S16). When it is determined that those two devices can communicate with each other a first encryption key is shared between the two devices (steps S18-S19). That shared first encryption key is then utilized in a second authentication operation (in steps S21-S23).

Thereby, in the claimed invention the second authentication unit carries out a second authentication with the receiving device for protecting copyright of the contents data to be transmitted through an encrypted radio communication using the first authentication key.

With such a claimed structure, even if a receiving device in the claimed invention does not have a copyright protection function, the receiving device can communicate with a

[1] See for example the present specification at page 3, lines 3-6.

transmitting device because the second authentication is carried out after the first authentication is carried out. If the second authentication was carried out before the first authentication was carried out the receiving device would not be able to communicate with a transmitting device.

As noted above, in the claimed invention a first authentication is carried out to determine whether two devices can properly communicate with each other, and then a second authentication can be carried out. As a non-limiting example that first authentication can be a Bluetooth encryption and the second authentication can be the DTCP authentication. Thereby, in the claims, when the Bluetooth authentication and key exchange is unsuccessful, then that second DTCP authentication is rejected.

Moreover, at least one of the second authentication unit and the second key exchange unit rejects its process of at least one of authentication and key exchange with the receiving device when at least one of the first authentication by the first authentication unit and the first key exchange by the first key exchange unit with the receiving device is unsuccessful.

Again with reference to Figure 2 in the present specification as a non-limiting example, the second authentication unit and the second key exchange unit 16 of the portable MPEG4 player (a transmitting device) 101 or the second authentication unit and second key exchange unit 26 of the portable viewer 103 (a receiving device) rejects its authentication and key exchange with the portable viewer 103 or the portable MPEG4 player 101 when the first authentication and first key exchange is unsuccessful.

As a non-limiting example the second authentication unit and second key exchange may be a Digital Transmission Contents Protection (DTCP) and the first authentication and first key exchange may be a Bluetooth authentication and key exchange.

In that non-limiting example, the DTCP authentication and key exchange unit 16 of the portable MPEG4 player 101 or the DTCP authentication and key exchange unit 26 of the

portable viewer 103 rejects its process of DTCP authentication and key exchange with a portable viewer 103 or the portable MPEG4 play 101 when the Bluetooth encryption cannot be realized. That is, if Bluetooth authentication and key exchange by the Bluetooth authentication and key exchange processing unit 13 with the portable viewer 103 or the portable MPEG4 play 101 is unsuccessful, then the DTCP authentication and key exchange is rejected.

Also, the second authentication unit and the second key exchange unit are located in an upper layer (e.g., DTCP layer) relative to a layer in which the first authentication and the first key exchange (e.g., Bluetooth layer) are carried out. Therefore, the DTCP authentication and key exchange unit controls sharing the encryption key and the DTCP layer based on a result of a security level in a lower layer than the DTCP layer.

The above-noted features reflected in the claims are believed to clearly distinguish over the applied art. That is, none of the Bluetooth reference, the 5C White Paper, or Morais discloses or suggests the above-noted feature of claim 1, and the similar feature in the other independent claims, that:

> wherein at least one of the second authentication unit and the second key exchange unit rejects its process of at least one of authentication and key exchange with the receiving device when at least one of the first authentication by the first authentication unit and the first key exchange by the first key exchange unit with the receiving device is unsuccessful.

The outstanding rejection relies on the Bluetooth reference to disclose a Bluetooth authentication and key exchange and relies on the 5C White Paper to disclose a second authentication and key exchange. However, clearly the 5C White Paper does not disclose or suggest rejecting its process if at least one of a first authentication by a first authentication unit and a first key exchange by a first key exchange unit with a receiving device is unsuccessful. The Bluetooth reference also does not provide any such teachings.

With respect to the above-noted feature the outstanding Office Action now cites Morais, and specifically states:

> Bluetooth and 5C does not specifically describe the condition wherein at least one of the second authentication unit and the second key exchange unit rejects its process of at least one of authentication and key exchange with the receiving device when at least one of the first authentication by the first authentication unit and the first key exchange by the first key exchange unit with the receiving device is unsuccessful. However, Morais discloses secure communication between at least one console-based systems communicating over wired or wireless interface with initially established secure communication links between one another so that data transferred data can be authenticated by the entities to ensure that a trusted entity did indeed send that particular data (see page 3, [0040]). Examiner further taken official notice that it is well known that if initial authentication fails, establishing connection between devices would have been broken down. Therefore, it would have been obvious to on of ordinary skill in the art at the time the invention was made to combine the teaching of first authentication taught by Bluetooth and second authentication taught by 5C with secure communication over the wireless link with initially established secure communication links taught by Morais to ensure that the initial authentication is securely connected to the trusted party.[2]

Applicants traverse the above-noted grounds for rejection in several aspects.

First, applicants note the above-noted grounds for rejection does not appear to be properly considering the claimed features. In the claims as written a second key exchange will be rejected if a first authentication or first key exchange is unsuccessful.

As discussed above in detail the claims recite first and second authentication units and first and second key exchange units. In the claims the second key exchange unit will reject its process if at least one of the first authentication and first key exchange is unsuccessful.

The basis for the outstanding rejection first cites Morais for such a proposition as Morais provides secure communication between two different network gaming consoles. Morais, however, merely indicates that transfer data can be authenticated by the entities to

[2] Office Action of April 25, 2007, pages 4-5.

ensure that a trusted entity did indeed send that particular data. Secure communications may or not involve encryption, which effectively renders the transmitted data blind to an observer. If encryption is used, it may occur before or after authentication.[3] Such disclosures in Morais are not at all directed to the claimed features as such disclosures in Morais do not indicate two different types of key exchanges, and wherein the second exchange will reject one of its processes if a first authentication or a first key exchange is unsuccessful. Morais, merely indicates an authentication prior to transferring data, and does not indicate that authentication involving a process such as in the second authentication unit or second key exchange as in the claimed invention.

Further, the proposition for which Official Notice is taken in the Office Action is hereby traversed and applicants require that prior art be cited for that proposition. Applicants also note the proposition for which Official Notice is taken, namely "that it is well-known that if initial authentication fails, establishing connection between devices would have been broken down", is an overly broad interpretation of the claims. That is, the claims do not merely recite an initial authentication to establish a connection between devices. As recited in the claims, if a specific one of a first authentication by a first authentication unit and a first key exchange by a first key exchange unit is determined to be unsuccessful, then at least one of a second authentication and a second key exchange unit rejects its process of at least one of authentication and key exchange. Again in the claims specific key exchange operations by a first key exchange unit and a first authentication unit must be successful prior to a second authentication unit and a second key exchange operation operating. The Official Notice is not at all directed to such specific features.

In such ways, applicants respectfully submit the current grounds for rejection citing Morais is traversed as Morais does not disclose the features noted above.

[3] Morais at cited paragraph [0040].

Applicants also submit the outstanding rejection is still not fully considering that in the claimed invention the second authentication is carried out after the first authentication and by using the first encryption key from the first authentication. That is, the claims recite a specific operation in which a first authentication is utilized to judge whether or not a receiving device is a device that is allowed to communicate with the transmitting device or for enabling the receiving device to operate as a device that is allowed to communicate with the transmitting device, and then a second authentication utilizes a first encryption key from the first authentication.

None of the Bluetooth reference, the 5C White Paper, nor Morais teach or suggest a first authentication and a second authentication being carried out in the specific order noted above, and particularly wherein that second authentication process will be rejected if one of the first key exchange or the first authentication is unsuccessful. In the claimed invention since a second authentication is carried out after the first authentication is carried out, a receiving device even without a copyright protection function can communicate with a transmitting device. None of the applied art to the Bluetooth reference, the 5C White Paper, nor Morais even allude to realizing such a result.

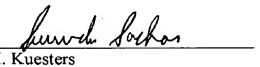
Applicants also note the Bluetooth reference, the 5C White Paper, and Morais do not teach or suggest being combined in any manner, particularly in the manner suggested in the Office Action. Each of those references discloses a single authentication, and none of the cited references disclose or suggest two such authentications as in the claimed invention. There is clearly no teaching in any of the cited references to be combined into systems with two such authentications as in the claimed invention.

In view of the foregoing comments, applicants respectfully submit that the claims as currently written clearly distinguish over the Bluetooth reference in view of the 5C White Paper and Morais.

As no other issues are pending in this application, it is respectfully submitted that the present application is now in condition for allowance, and it is hereby respectfully requested that this case be passed to issue.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Surinder Sachar
Registration No. 34,423

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 03/06)

I:\ATTY\SNS\21's\213200\213200US-AM-DUE-7-25-07.DOC